AIR WAR COLLEGE

AIR UNIVERSITY

CYBERPOWER AS A COERCIVE TOOL IN 2035

by

John D. Bedingfield, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

15 February 2011

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the United States Government, the Department of Defense, or the United States Air Force. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States Government.

Contents

Disclaimer i

Contents ii

Biography iii

Abstract iv

Introduction and Overview 1

Technological Advancements Creating a Unique Environment in 2035 3

Cyber as a Unique Domain 4

Cyber As a Coercive Force 7

Criticisms of Cyber Coercion 9

Factors Improving Cyber’s Coercive Power 12

Recommendations for Future Investment 14

Summary and Conclusion 15

Bibliography 17

Endnotes 20

Biography

Lieutenant Colonel John Bedingfield has 16 years of Department of Defense acquisition program management experience. In 1993 he received his undergraduate degree from Auburn University in Aerospace Engineering, and was commissioned through the Air Force Reserve Officers Training Corps program. Since entering Active Duty, his assignments have included managing various types of acquisitions in areas such as aircraft communication and navigation modification, black-box airborne Signals Intelligence, logistics information system technology, the Air Force Portal, and command and control systems. He has served in System Program Offices at Aeronautical Systems Center, Electronic Systems Center, and the Missile Defense Agency. He also served on Air Force / Secretary of the Air Force Headquarters (AF/SAF AQ) in the Air Force Program Executive Office for Command and Control and Combat Support Systems. His most recent assignment was as the Deputy Program Manager of the Global Combat Support System – Joint, a Joint Acquisition Category IAC information technology development program at the Defense Information Systems Agency. He is an Acquisition Professional Development Program Level-III certified program manager and holds a Masters of Science degree from the Air Force Institute of Technology in Research and Development Management.

Abstract

Although coercion by cyberpower alone may be limited today, if appropriate steps are taken, by the year 2035 cyberpower will be a useful coercive instrument of power. This essay explores the reasons why cyberpower is not coercive today, and ways it may become more coercive in the future. The cyber attacks employed against Estonia and Iran provide evidence cyberpower is currently not coercive, as do today's unique cyber attributes. Subsequently, many experts criticize the coercive ability of cyber tools, arguing the ability to quickly deploy countermeasures to a cyber attack, imprecise cyber tools, and lack of attribution; are all reasons why cyber may not be coercive. However, as technology continues to improve and proliferate, and cyber tools are further explored, just as in the early days of airpower, cyberpower may provide increasingly precise tools. Furthermore, increased attribution and weapons providing repeatable and reliable effects may emerge from a concerted investment effort. Therefore, the essay concludes, the United States should invest in forensics, repeatable tools, defense, and cyber models, simulations, and analysis to ensure dominance is maintained as cyber progresses toward a more coercive power.

Introduction and Overview

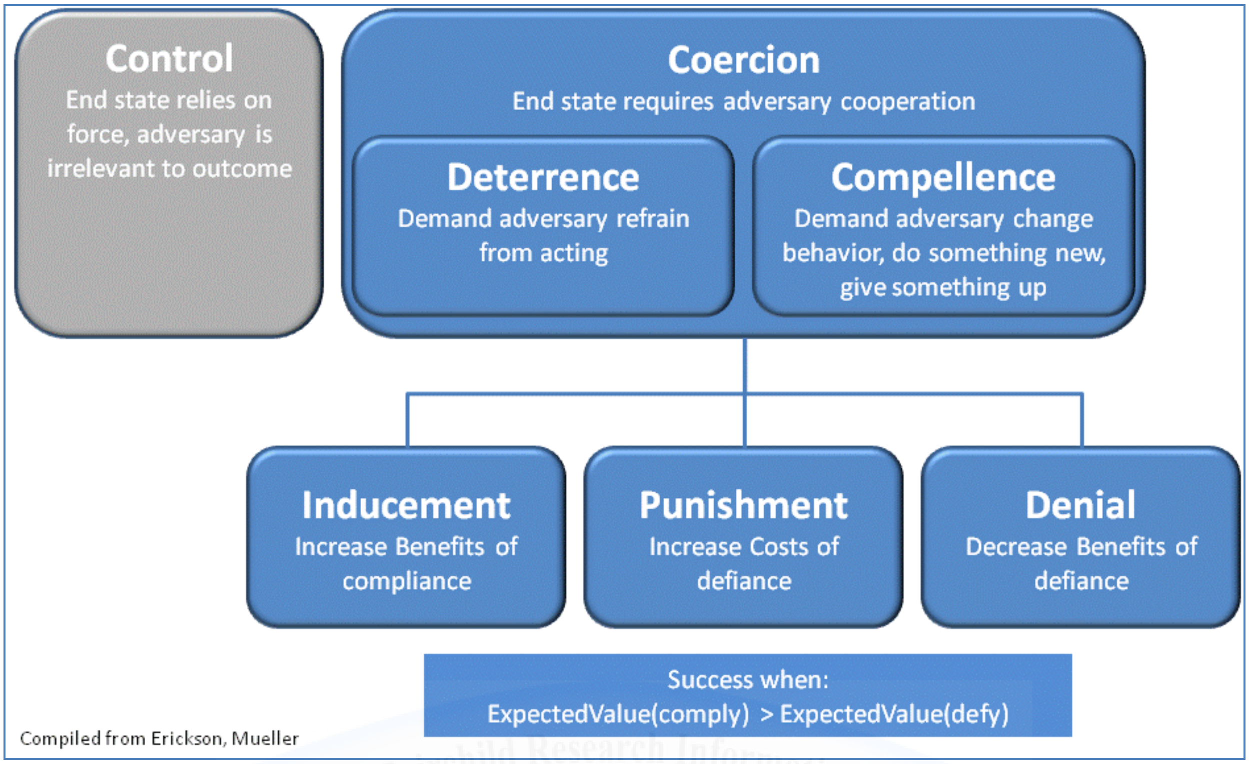
This essay explores the coercive force of cyberpower. Although coercion by cyberpower alone may be limited today, by the year 2035 cyberpower will be a useful coercive instrument of power. To describe the way cyberpower might become a coercive force, this essay is structured into three major parts. First, an overview provides key definitions, coercion concepts, and a coercion framework. Second, the current unique attributes of cyberpower are explored to provide the reader with a set of key cyber attributes applicable to cyber coercion, followed by some of historical examples, and current arguments to explain why cyber is not a coercive force today. Finally, counterarguments are proposed, and the paper concludes with a few conditions that might indicate how cyberpower will become more coercive, concluding with some recommendations.

Cyberspace is increasingly important and complex. By one estimate, 95 percent of all United States government and military communications traffic is carried on private commercial communication lines.[1] In addition, 97 percent of the United States Gross Domestic Product (GDP) exists as "cybercash", or virtual money, represented only by ones and zeros in cyberspace.[2] Cyberspace increasingly defines and controls key services such as communications, electricity, banking, military command and control, entertainment, information and news, supply chain management, business to business transactions, and government services. In fact, it is hard to imagine a single organization within the United States Air Force that could function efficiently for more than a day without access to cyberspace.

For purposes of this essay, cyberspace is defined as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."[3] The definition of cyberpower is "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power," where operational environments include air, land, sea, and cyberspace.[4] Furthermore, for the purposes of this essay, the "coercer" is the actor attempting to coerce another, and the "target" is the subject of the coercion attempt.

Figure 1 below provides an overview of the coercion framework selected for this essay. Coercion is differentiated from "control" because coercion requires willing adversary cooperation, and control does not. Furthermore, coercion consists of both deterrence and compellence, with their associated definitions depicted in Figure 1. Since much has been written regarding cyber deterrence, this essay will focus more on compellence, but will not exclude deterrence considerations. Also, from Figure 1, coercion can be achieved using three methods; inducement, punishment; and denial. Since coercion requires a rational decision by the target of the coercion, a cost benefit calculus is provided at the bottom of Figure 1. If the target perceives the value of complying to be greater than the value to defy, the target is coerced. For each method of coercion, Figure 1 describes the aspect of the target calculus impacted. For example, denial affects the benefits of defiance by reducing these benefits.

This taxonomy is usually not so clear in the "real world." For example, one state may attempt to coerce another state by simultaneously using deterrence, compellence, inducement, punishment, and denial. Subsequently, given a specific "real world example" the type of coercion may be difficult to classify. However, the intent of the framework is not to provide a method to classify all cyber incidents, but rather to provide a mental framework with which to discuss cyber coercion in general terms. To provide a more complete framework, some differences between today and 2035 are described.


Control
End state relies on force, adversary is irrelevant to outcome
Coercion
End state requires adversary cooperation
Deterrence
Demand adversary refrain from acting
Compellence
Demand adversary change behavior, do something new, give something up
Inducement
Increase Benefits of compliance
Punishment
Increase Costs of defiance
Denial
Decrease Benefits of defiance
Success when:
ExpectedValue(comply) > ExpectedValue(defy)

Compiled from Erickson, Mueller

Figure 1: Coercion Framework

Technological Advancements Creating a Unique Environment in 2035

Key technologies are advancing at exponential rates, and will create a unique strategic environment in 2035. Hardware, bandwidth, nanotechnologies, and biotechnologies are appearing and available at accelerating exponential rates.[5] As a result, prices for new and advanced technologies continue to decrease, proliferation of these technologies continues to expand, barriers to entry continue to decrease, and as Thomas Friedman predicted, globalization expands.[6] Subsequently, capabilities once only available to powerful, well financed states are now increasingly available to small groups and even individuals.

Therefore, several aspects of human life in 2035 may look unrecognizable from today's perspective. For example, given the rapid pace of technological innovation, as well as decreasing prices, it is conceivable that every manufactured or processed item (food package, clothing, accessory) may have an implanted, networked chip, and may provide services for tracking, information, and intelligence. These devices may provide instantaneous, integrated information to the user, but also may collect information on the daily activities of the user, making this information available for tailored experiences, data mining, or nefarious uses. Furthermore, information increasingly becomes a commodity in 2035, accessible to all through various methods and formats, and trending toward cyber omniscience: "the ability to conduct comprehensive intelligence collection on any [potentially] threatening cyberspace activity followed by near-simultaneous processing, exploiting and disseminating of the information."[7] Subsequently, cyber "Familiars" or "Digital Twins" will be important to assist users to sift through large volumes of data, or provide decision aids.[8] Furthermore, as mankind nears Kurzweil's *Singularity*[9], cyber coercion may be required at the state, group, individual, and artificial intelligence levels; requiring deterrence and compellence of both man and machine. To further determine how the cyber domain might look different in 2035, it is first useful to consider the unique aspects of the cyber domain today.

Cyber as a Unique Domain

At present, cyberspace is recognized as a unique domain with singular attributes.[10] These attributes describe the current aspects of cyber tools, but do not describe future implications for cyber tools, which will be explored later in this essay. There are seven unique characteristics of current cyber tools that should be considered.

First, cyber tools are unique because they are highly perishable, rely upon system vulnerabilities which limit them to single-use use weapons and provide confusion between intelligence and attack.[11] Perhaps more than other weapons, cyber weapons rely upon system vulnerabilities to exploit. Consequently, many cyber tools used for attack are limited to a single use, or at best only a few uses. Once the tool has been used, the target of the attack can identify the vulnerability and take measures to correct it. Even if a tool has not been used, it is still possible for the vulnerability to be discovered and corrected, rendering the tool useless. As a result, cyber tools have very limited life spans. Therefore, attack options available to a commander may change from day to day, and from microsecond to microsecond as systems continually patch vulnerabilities.

Furthermore, to gain an accurate understanding of current system vulnerabilities, intelligence gathering is critical, both Computer Network Exploitation (CNE) and Battle Damage Assessment (BDA). In some cases the same cyber tools can be used for intelligence collection and attack. This adds confusion over cyber intentions, and can expose vulnerabilities, which may then be corrected, negating the effect of the cyber tool. In addition, attacks can take place at near light speed, or lay dormant in wait at the risk of being rendered useless before they can be employed. These characteristics can dramatically shorten the commander's observe-orient-decide-act (OODA) loop.[12] Therefore, cyber weapons, because they are based on vulnerabilities, are highly perishable and present complications to the commander attempting to employ cyber tools.

A second unique cyber attribute is the difficulty of attribution, and consequently, deterrence.[13] Attributing cyber attacks is difficult because attackers can spoof identities and tamper with electronic evidence. Furthermore, some cyber attacks are indistinguishable from standard system errors.

A leading cyber strategy expert from RAND, Dr. Martin Libicki, describes the likelihood that an attack is visible as a function of the visibility of the effects, and the likelihood the effects will be assigned to a cyber attack.[14] Regardless of whether attribution is difficult because the coercer has taken steps to avoid detection, or the attack has been misattributed to another actor (or system error), attribution challenges lead to deterrence challenges. If the attacker is confident their identity cannot be known, or will be misidentified, they may also be confident retribution, if any, will be difficult. Therefore, in the attacker's calculus, if there is little risk of retribution, there is little risk the attack will result in unacceptable costs.

A third unique cyber attribute is the strength of offense over defense.[15] In the other domains, defense normally has the advantage. In cyber, the cost of attack is relatively low compared to the cost to defend.[16] Therefore, over time, the offense can wear down the defense, or this cost-imposing strategy may cause the defense to expend disproportionate resources.

A fourth unique cyber attribute is one it shares with early airpower; cyber can operate at the tactical, operational, and strategic levels simultaneously, however cyber effects are sometimes uncertain.[17] Because cyberspace consists of interconnected networks and systems, a change in one aspect may cause unintended effects in other parts of the "system" at all levels (many of which cannot be modeled or predicted). Therefore, cyber tools may not always be precise, and collateral effects may be hard to estimate. Similarly, obtaining cyber Battle Damage Assessment (BDA) may be more difficult than obtaining BDA in other domains due to less certain cyber effects.

Fifth, cyberspace barriers to entry are low, so anyone, including non-state actors and even individuals can become major players in the cyber domain.[18] Dr. Libicki lists only five requirements: "talented hackers, intelligence on the target, exploits to match the vulnerabilities found through such intelligence, a personal computer of any comparable computing device, and any network connection."[19] Since the entry costs are so low, counter proliferation is exceedingly difficult.[20] Therefore, once a vulnerability is exploited, it may be possible for many different actors to quickly gain access to tools used to exploit any real or perceived vulnerability. These tools may present strategic advantage, and coercion options once only available to the most powerful state actors may now also be available to individuals, presenting a myriad of asymmetric threats to challenge cyber defenses.

A sixth unique cyber characteristic involves the difficulty to obtain dominance.[21] In fact, cyber dominance may not be possible, allowing only limited and transient superiority in and over specific areas. Similar to airpower, cyberpower does not permit the occupation of territory.[22] Furthermore, cyberpower is limited to a discrete segment of cyberspace, for a limited time (perhaps measured in nanoseconds). As previously discussed, the rapid correction of vulnerabilities presents additional challenges to maintaining cyber dominance.

The final characteristic is that cyber is today primarily a weapon against cognition.[23] Cyber is primarily a man-made domain.[24] Although some initial indications of physical destruction are emerging,[25] to date no one has been killed by a cyber attack.

Cyber As a Coercive Force

Considering the current unique cyber attributes and limitations, today cyberpower is not coercive by itself. However, it may be possible by 2035 for cyber to reach a tipping point where cyber becomes coercive, similar to the rise of airpower over time. This section will begin by exploring two current historical examples, Estonia and Iran, which elucidate the limitations of cyber coercion[26], followed by some generic coercion considerations, a few common criticisms of cyber coercion, and some possible ways cyber might become coercive in 2035.

In 2007, Estonia relocated a statue, “The Bronze Soldier of Tallinn,” dedicated to former Soviet Union World War II war dead.[27] Although the resulting April 2007 Distributed Denial of Service (DDoS) attacks were never officially attributed to the Russian Government, most sources attribute the attacks to Russian patriotic sympathizers: one Estonian has been convicted in the attacks, [28]and at least one Russian Nashi youth leader, Konstantin Goloskokov, who was also the assistant to State Duma Deputy Sergei Markov, has admitted involvement.[29] Regardless of who was responsible, and although the DDoS attacks disrupted access to Estonian banks, parliament, ministries, and communication outlets, in the end the attack did not coerce the Estonian Government to replace the statue.

An even more recent example of the limitations of cyber coercion is the 2010 Stuxnet attack on the Iranian nuclear development program.[30] Targeting the uranium enrichment centrifuges located at Natanz for what many believe to be a clandestine nuclear weapon development program, the Stuxnet virus attacked the Siemen's frequency converters, causing the centrifuges to spin faster than intended, causing damage.[31] Although many nations desire to disrupt the Iranian nuclear program, and although the attack was rather complex, exploiting four "zero day" vulnerabilities (vulnerabilities previously unknown), the attack has not yet been attributed. Again, regardless of the attacker, the end result may have delayed Iran's nuclear program, but did not convince the Iranian Government to stop spinning the centrifuges.[32]

One compelling theory for why previous cyber attacks have not yet yielded the desired coercion: the attacker has not yet attacked all three aspects of Clausewitz' trinity.[33] This theory posits coercion is successfully only when all three elements of Clausewitz's paradoxical trinity are attacked: the people, the government, and the military. Applying this theory to the two historical examples seems to reach similar conclusions. Although the attack in Estonia targeted the Estonian Government, and the people to a lesser extent, the military was not directly targeted. Similarly, the Iranian Stuxnet attack was very tactical, and did not directly target the will of the people, the rationality of the Iranian Government, or the Iranian military. Consequently, in both cases at least one element of the Clausewitzian trinity was not impacted, subsequently coercion was unsuccessful.

Furthermore, referring back to Figure 1, successful coercion consists of "capability X will X perception" in the perceived cost-benefit calculus of the coercion target.[34] For successful coercion, the coercer must have the capability to induce, punish, or deny, and the will to use its capabilities. In addition, the coerced must perceive the attacker's capability and will in a way that creates the desired cost-benefit. Even if an individual has the capability and the will to coerce a state, the state must correctly perceive the individual has the capability and the will, or else the state will not be coerced, perhaps out of ignorance if for no other reason. Given the difficulties with cyber attribution, and the perishability of cyber tools, cyber coercion today is a very difficult proposition.

Criticisms of Cyber Coercion

Many academics view cyberpower playing only a supporting role to the other instruments of national power (diplomatic, informational, military, economic), or as a supporting domain to the other domains.[35] Several arguments, including the ease of countermeasures to a cyber attack, imprecise cyber tools, and lack of attribution frame their perspective. Each of these arguments will be presented and countered.

First, one reason critics believe cyberpower cannot be coercive is because countermeasures can be quickly created. For example, for a state to coerce another state, the threat must be made known in an understandable way. Once the coercion target is aware of the threat, associated vulnerabilities are revealed, and actions can be taken to create countermeasures to correct the vulnerability, negate the attack, or reduce the cost of the attack.[36] Therefore, proponents of this argument think cyberpower cannot be coercive as the very act of communicating the capability allows the coerced to discount or counter the foundation of the coercion.

The ability to quickly mount countermeasures is a cogent argument as long as the underlying assumptions remain valid. This argument assumes that communicating coercive intent also gives away the underlying attack vector. While this may be true in some cases, precise communication, which is understood by the coerced without revealing specifics, may ameliorate some of these risks. In addition, this argument assumes the cyber quiver will remain as sparse as it is today. As technology continues to improve, and as cyber prowess increases, it may be possible to create a "system" capable of recommending and executing multiple attack vectors for the commander, to reduce the effectiveness of countermeasures.

A second argument against cyber as a coercive force predicts the imprecision of the current tools will make cyber effects difficult to achieve.[37] As previously described, today's cyber tools are imprecise, and collateral effects are often difficult to predict given the interconnected, and ever changing, aspect of cyberspace. Therefore, this argument posits coercion will be difficult since linking a specific coercive cyber action with a specific effect is difficult. Furthermore, although the coercer may be able to link the action with the effect, if the target cannot make the same linkage, they will not be aware they are being coerced, may not engage in a rational coercion calculus, and probably will not respond as desired. For example, if a target misreads a coercive attack as simply a system error, the target will not perceive the coercion, and not respond to the coercer's demands.

Again, if the underlying assumptions remain valid, this argument is very persuasive. However, as improved cyber technologies become available, it may be possible to increase the precision of cyber tools. For example, in the early days of airpower, attacks were also very imprecise. Over time, new technologies became available, such as the Norton Bomb Sight and precision guided weapons, which allowed ever increasing levels of precision. Consequently, if in 1920 the United States had attempted to threaten to sink another state's Navy using only airpower, the United State's lack of precision capabilities would likely have undermined its coercive intent. However, after Brig Gen Billy Mitchell demonstrated the sinking of the battleship *Ostfriedsland* on 21 July 1921, and subsequent technological improvements in the following decades, no nation doubts the United State's precision bombing capabilities in 2020. Although speculative at this point, a similar path may be possible for cyber tools. Over time, innovation by cyber warriors may increase accuracy, contain damage, and permit more precise effects.

The third argument against a coercive cyberpower hinges on the difficulty of attribution. Currently attribution in the cyber domain is difficult, and so is deterrence. Since attributing attacks is difficult, the "perception" of the effects of an attack, or an impending attack, by the coerced becomes difficult as well. Similar to the argument regarding imprecision, if the mind of the target is unable to tie an event to the coercer, it will be difficult to affect the target's decision calculus, and thus coercion will fail.

Again, as with the other arguments, over time technological improvements may negate some of these underlying assumptions. For example, forensic capabilities will likely improve, and so will attribution. Once attribution improves, the target will be able to link the coercion to specific events. However, technological improvements alone may not be required. A state may choose to divulge their actions to ensure the target will "connect the dots." Although a declaration of responsibility does not always guarantee all parties will perceive the connection, a state may choose to publicly state their actions to manipulate the target's perceptions.

Furthermore, the ability of a target to convincingly prove the linkages between the coercer and the coercive vectors may not always be required. For example, although Estonia has not been able to prove Russia was behind the April 2007 cyber attacks, if Estonia has enough evidence to convince itself Russia orchestrated the attacks, perfect attribution may not be required to push Estonia to take action.

Factors Improving Cyber's Coercive Power

Therefore, after considering the arguments and counterarguments regarding the coercive aspects of cyberpower, transparency, improved attribution, and technological improvements seem to increase cyber's coercive power. In addition, several key indicators may elucidate the increase in cyberpower's coercive effects including the increase in transparency and attribution, better cyber technology, and an enhanced ability to simultaneously target all aspects of Clausewitz's paradoxical trinity. With improved transparency and attribution, an actor could improve punishment and denial, and deterrence in general.

Furthermore, deterrence can be increased if bad actors understand they are being monitored 24x7x365. For example, the *Angel Fire* program provides a tactical battlefield commander with near continuous surveillance of the battlefield and TIVO-like ability to record and "rewind" the battlefield.[38] Likewise, extensive video cameras in major cities such as London might deter crime if the criminal assumes they are under constant surveillance and will be caught.[39] If a similar program existed for cyberspace, it might deter those who otherwise believe they can act with impunity, or at least collect the evidence required for prosecution, retribution, or private negotiations.[40]

Over time, influence operations and other forms of cognitive influence may become easier as technologies improve, costs are reduced, and more people are able to "plug-in." As more people have access and use the cyber domain, it will inculcate their lives. Increase in usage, and reliance upon, the internet, cell phones, and satellite radio and television, all provide avenues to conduct influence operations. As technology continues to increase and Cyber Familiars become pervasive, additional opportunities open for coercion and influence. Consequently, trust in the information presented continues to be a major issue.

Another indicator cyberpower may increase its coercive abilities is the recent demonstration of the cyber domain influencing the physical domain. In March 2007, the Departments of Homeland Security and Energy conducted a test where researchers attacked the control mechanism of a power generator, causing physical damage and failure.[41] Although some of these specific vulnerabilities are no doubt being addressed, the test showed that cyber tools alone can reach beyond cyberspace into the physical domain.

Further, as the world becomes increasingly reliant upon cyberspace, and even electricity in general, the tie between the cyber and physical domains will grow stronger, with ever increasing vulnerabilities. Forstchen's cautionary tale, *One Second After*, depicts a world immediately after an Electromagnetic Pulse attack destroys almost all electrical devices in the United States. Although not a cyber attack, effects could be similar. For example, with a loss in refrigeration, insulin supplies can run out putting diabetics at risk. Indeed, all the major comforts of modern life such as air conditioning, running water and sewer, and communications, could be disrupted for extended periods, even years. Since all of these technical innovations have expanded mankind's life expectancy, the removal of these items subsequently shortens life expectancy, and the very young and the elderly are likely the first casualties. As the world increasingly becomes more interconnected, it is not hard to imagine a blurring between the cyber domain and the physical domain, and the effects caused by the interaction between the two domains.

Recommendations for Future Investment

Given the increasing importance of cyberpower, and the possibility it may become coercive by 2035, the United States Air Force should consider some investments to help shape the cyber future. Several investment efforts are currently ongoing in both the Air Force Research Laboratory, and in the commercial world, however increased Defense Department cyber investments may help the United States reach key tipping points sooner than its adversaries.

First, the United States should continue to invest in cyber forensics and attribution capabilities.[42] Since so many aspects of cyber coercion hinge on the ability to immediately and properly attribute an attack, and since forensic capabilities are critical to attribution, these two areas represent keys to future cyber coercion efforts.

Furthermore, overcoming one of today's critical cyber limitations, tool perishability, is another important investment area. Once repeatable cyber weapons are available, an array of options becomes available to the commander. In cyber, repeatable may not entail using the same tool, in the exact same way, time and time again. Repeatable in the cyber realm may mean having an arsenal of similar tools, against similar targets, that all produce the same effect, and can be used in concert with each other so that they remain viable tools. Regardless of the mechanism, developing repeatable tools may be one key step toward cyber coercion.

Likewise, cyber defense will continue to be a critical capability.[43] Even though cyber offence is currently stronger then defense, it is conceivable defense will someday catch up; regardless some defense will always be required. Therefore, additional defensive capability including active defenses operating at the speed of light, as well as agile, resilient networks will be critical. Complicating the investment strategy will be the amount of defensive cyber investment in the commercial world, and the subsequent proliferation of those technologies. However, as defensive capability is an every changing cat-and-mouse game, investment in this area will ensure the United States maintains its competitive edge.

Other key supporting capabilities include models, simulations, and analysis.[44] Just as forces in other domains use modeling and simulation, wargames, and exercises to test and evaluate new ideas, cyber warriors should be afforded the same tools and opportunities. Since cyber capabilities and strategies are rapidly evolving, it is perhaps more important now to provide mechanisms that allow warriors to experiment with new ideas.

Summary and Conclusion

Although cyberpower is not coercive by itself today, if appropriate steps are taken, cyberpower may be reliably coercive by 2025. The cyber attacks employed against Estonia and Iran provide evidence cyberpower is currently not coercive, as do today’s unique cyber attributes. Currently cyber attribution is difficult, as is deterrence. Furthermore, current cyber tools are one-use, or limited use only, since they are based on exploiting known vulnerabilities which can be quickly corrected. Subsequently, many experts criticize the coercive ability of cyber tools, arguing the ability to quickly deploy countermeasures to a cyber attack, imprecise cyber tools, and lack of attribution; are all reasons why cyber may not be coercive. However, as technology continues to improve and proliferate, and cyber tools are further explored, just as in the early days of airpower, cyberpower may provide increasingly precise tools. Furthermore, attribution and repeatable weapons may emerge from a concerted investment effort. Therefore, the United States should invest in forensics, repeatable tools, defense, and cyber models, simulations, and analysis to ensure dominance is maintained as cyber progresses toward a more coercive power.

Bibliography

Air Force Doctrine Document (AFDD) 3-12. *Cyberspace Operations*, 15 July 2010.

Barnes, Ed. "Mystery Surrounds Cyber Missile That Crippled Iran's Nuclear Weapons Ambitions." Fox News .com, 26 November, 2010. http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/ (accessed 29 November, 2010).

Benson, Pam. "Computer virus Stuxnet a 'game changer,' DHS official tells Senate." Cable News Network .com, 17 November, 2010. http://articles.cnn.com/2010-11-17/tech/stuxnet.virus_1_stuxnet-nuclear-power-plants-target?_s=PM:TECH (accessed 13 December, 2010).

British Broadcasting Corporation. "Estonia fines man for 'cyber war'." 25 January, 2008. http://news.bbc.co.uk/2/hi/technology/7208511.stm (accessed 12 December, 2010).

Carr, Jeffrey. *Inside Cyber Warfare: Mapping the Cyber Underworld*. Sebastopol, CA: O'Reilly Media, Inc., 2010.

Chilton, General Kevin P. "Cyberspace Leadership: Towards New Culture, Conduct, and Capabilities." *Air & Space Power Journal* Volume XXIII, no.3 (Fall 2009): 5-10.

Clover, Charles. "Kremlin-backed group behind Estonia cyber blitz." *Financial Times .com*, 11 March 2009. http://www.ft.com/cms/s/0/57536d5a-0ddc-11de-8ea3-0000779fd2ac.html#axzz17wANf3yT (accessed 12 December, 2010).

Convertino II, Sebastian M., Lou Anne DeMattei, and Tammy M. Knierim. *Flying and Fighting in Cyberspace*. Montgomery, AL: Air University Press, 2007.

Evron, Gadi. "Authoritatively, Who Was Behind Estonian Attacks?" darkreading.com, 17 May 2009. http://www.darkreading.com/blog/227700882/authoritatively-who-was-behind-the-estonian-attacks.html (accessed 12 December 2010).

Evron, Gadi. "Battling Botnets and Online Mobs: Estonia's Defense Efforts during the Internet War." *Georgetown Journal of International Affairs*, Winter/Spring 2008: 121-126. http://www.ciaonet.org/journals/gjia/v9i1/0000699.pdf (accessed 12 December, 2010).

Friedman, Thomas L. *The World is Flat: A Brief History of the Twenty-First Century*. New York, NY: Farrar, Straus and Giroux, 2005.

Garreau, Joel. *Radical Evolution: The Promise and Peril of Enhancing our Minds, Our Bodies – and What It Means to Be Human*. New York, NY: Doubleday, 2005.

Gloystein, John W. "Cyberdeterrence in 2035: Redefining the Framework for Success." Research Report. Maxwell AFB, AL: Air War College, 2010.

Jensen, William P. "Toward Cyber Omniscience: Deterring Cyber Attacks by Hostile Individuals in 2035." Research Report. Maxwell AFB, AL: Air War College, 2010.

Kramer, Franklin D. "Cyberpower and National Security: Policy Recommendations for a Strategic Framework." In *Cyberpower and National Security*. Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington DC: Potomac Books, 2009.

Kuehl, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem." In *Cyberpower and National Security*. Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington DC: Potomac Books, 2009.

Kurzweil, Ray. *The Singularity is Near: When Humans Transcend Biology*. New York, NY: Penguin, 2005.

Lawless, Jim. "British Study Says CCTV Cameras Don't Deter Crime." *Associated Press*, 6 February, 2009. http://www.securityinfowatch.com/CCTV+%2526+Surveillance/british-study-says-cctv-cameras-dont-deter-crime (accessed 13 December, 2010).

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Santa Monica, CA: RAND Corporation, 2009.

Lonsdale, David. J. *The Nature of War in the Information Age: Clausewitzian Future (Strategy and History)*. New York, NY: Frank Cass, 2004.

Maclean, William. "Stuxnet study suggests Iran enrichment aim: experts." *Reuters.com*, 16 November, 2010. http://www.reuters.com/article/idUSTRE6AF2F320101116 (accessed 13 December, 2010).

Meserve, Jeanne. "Sources: Staged cyber attack reveals vulnerability in power grid." *Cable News network .com*, 26 September, 2007. http://edition.cnn.com/2007/US/09/26/power.at.risk/index.html (accessed 13 December, 2010).

Mueller, Karl. "The Essence of Coercive Airpower: A Primer for Military Strategists," *Air and Space Power Journal Chronicles* (17 September 2001).

O'Neil, William D. "Cyberspace and Infrastructure" In *Cyberpower and National Security*. Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington DC: Potomac Books, 2009.

Rattray, Gregory J. *Strategic Warfare in Cyberspace*. Boston, MA: Massachusetts Institute of Technology, 2001.

Reuters. “Iran says cyber foes caused centrifuge problems.” Reuters.com, 29 November, 2010. http://www.reuters.com/article/idUSLDE6AS1L120101129 (accessed 13 December, 2010).

Sharma, Amit. “Cyber Wars: A Paradigm Shift from Means to Ends.” *Strategic Analysis* 34, no. 1 (January 2010): 62-73.

Starr, Stuart H. “Toward a Preliminary Theory of Cyberpower.” In *Cyberpower and National Security*. Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz. Washington DC: Potomac Books, 2009.

United States Air Force Chief Scientist. *Report on Technology Horizons: A Vision for Air Force Science & Technology During 2010-2030*. Washington, DC, 2010.

William A. Owens, Kenneth W. Dam, and Herbert S. Lin, eds. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities*. Washington, D.C.: The National Academies Press, 2009.

Zachary, Stacia. “Angel Fire surveillance a key tactical asset.” *Team Eglin Public Affairs*, 27 January, 2009. http://www.eglin.af.mil/news/story.asp?id=123132586 (accessed 13 December, 2010).

Endnotes

[1] Lonsdale, pg. 11

[2] Lonsdale, pg. 11

[3] Joint Publication 1-02. For the purposes of this essay, this definition is adequate. However, cognition seems to be an important concept missing from the current definition. It is important to include cognition in the cyber definition since cyber is uniquely equipped to influence the systems that make up an enemy's OODA loop, the enemy's cognition, which impacts coercion.

[4] Kuehl, pg. 38. Here "operational environments" means air, land, sea, as well as cyber. "Instruments of power" include, in the author's terms, political, informational, military, and economic.

[5] Rattray, pp. 54-56. For hardware acceleration see Moore's Law: Kurzweil, Kindle pp. 1286ff (I think these are actually sentence numbers) and Garreau, Kindle pp. 868ff. Software also continues to progress, but at a slightly slower rate: Garreau, Kindle p 1355; also see Marvin Minsky's comments that we are bad at writing software; see also Garreau, Kindle p 3877, Lanier believes software does not follow Moore's law; Garreau, Kindle p. 3934, Quote from Vernor Vinge, "If we are still plunking around with software in 2012 or 2015, that would be a really bad sign for people who expect a real-soon-now Singularity." Garreau, Kindle p. 3940, Kurzweil's claim that software is not moving as fast as hardware, but is doubling every six months.

[6] Friedman

[7] Jensen "Toward Cyber Omniscience". A good definition at Page 7. Also, good discussion through out of the implications.

[8] Gloystein. Gloystein also discussed the need to deter Cyber Familiars.

[9] Kurzweil's singularity is "a future period during which the pace of technological change will be so rapid, its impact so deep, that human life will be irreversibly transformed." (Singularity, Kindle pp 404-417) Kurzweil predicts a point, a singularity, where computing power and computing intelligence surpasses the abilities of the human mind. From this point it will be increasingly difficult for humans to predict or fathom technological innovations beyond the singularity.

[10] Air Force Doctrine Document (AFDD) 3-12. Pg2,3

[11] Libicki, pp. 18, 19, 56-59.

[12] Starr, pg 57. AFDD 3-12, pg. 30.

[13] Libicki, pp 40-52. AFDD 3-12, pg. 10

[14] Libicki, pg. 92

[15] Starr, pp. 55, 56

[16] Libicki, pg. 33

[17] Libicki, pp 52-56

[18] Rattray, pp.137-139. AFDD 3-12, pg. 3, 4. Kramer, pg 5.

[19] Libicki, pg 59

[20] Rattray, pp 139-142

[21] AFDD 3-12, pg. 2. Kramer, pp. 12, 13.

[22] Libicki, pg. 119

[23] Libicki, pg. 119, 172

[24] Rattray, pg 65. Libicki, pg. 11. As an aside, one could argue cognition is not universally man-made. However, the rest of cyberspace is man-made, as opposed to the other domains which exist naturally. Therefore, to be complete, cyberspace is 'primarily' man-made.

[25] Meserve "Sources: Staged cyber attack reveals vulnerability in power grid." See also O'Neil, pp. 126-130. Note O'Neil believes a cascading electrical grid failure in the U.S. is unlikely, pg. 122, because the effects will disperse and the North American regions are somewhat isolated.

[26] An Interview with Dr. Sheldon pointed this out with great clarity, and he offered the examples presented in this section, along with several other examples.

[27] Carr, pg 3. See also Evron. These are also references for this entire para.

[28] BBC, "Estonia fines man for 'cyber war'"

[29] Carr, pg. 3. See also Clover, Evron "Authoritatively…", and Evron "Battling Botnets..."

[30] Barnes

[31] Barnes, Maclean
[32] Reuters "Iran says cyber foes caused centrifuge problems". As an interesting aside, the Stuxnet virus may not be finished, and may not be as precise as desired. Apparently, some in the U.S. are worried that the virus may spread and cause damage to U.S., or allied, facilities as well. See Benson "Computer virus Stuxnet…"
[33] Sharma
[34] Air War College Seminar discussions.
[35] For example, Libicki's restriction of operational cyberwar, or support to military forces, versus strategic cyberwar. Libicki, pg 137. For operational cyberwar definitions and considerations see pp 139-142
[36] Libicki, pp. 56-59.
[37] Libicki, pp. 52-56.
[38] Zachary "Angel Fire surveillance a key tactical asset"
[39] See Lawless. A study was conducted that indicated the London cameras may not be providing as much deterrence as originally advertised.
[40] Re: private negotiation. See Libicki, pp. 128, 129. However, in some cases, Libicki argues such publicity may work against the coercer. If the target of the coercion is afraid of the effects of public opinion, they may be willing to make concessions to handle the coercion privately, without involving their populace. This may be especially true if a state under coercion has tentative control over their populace, and if they feel a cyber attack may induce undue panic in the populace, making it more difficult to govern.
[41] Meserve "Sources: Staged cyber attack reveals vulnerability in power grid." See also O'Neil, pp. 126-130. Note O'Neil believes a cascading electrical grid failure in the U.S. is unlikely, pg. 122, because the effects will disperse and the North American regions are somewhat isolated.
[42] Kramer, pg 16.
[43] Libicki, pp 173, 174
[44] Starr, pg 81